ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Information Security in an Organization

Mohammed Mahfouz Alhassan[a*], Alexander Adjei-Quaye[b]

[a,b]*Zhejiang Normal University College of Mathematics, physics & Information Engineering, 688 tying bin road,321004, Jinhua –Zhejiang Province, CHINA.*

[a]*Email: mmalhassan@tamalepoly.edu.gh*

[b]*Email: adjeiquayealexander@gmail.com*

Abstract

Information security is one of the most important and exciting career paths today all over the world. Information security simply referred to as InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical data, with knowledge of information security we are confident that our data is protected and also assured of the safety of our data and ensure that the value of our organizations maintained. But this is not the only explanation experts have given, information security is the life savior of organizations all over the globe. So people in this field can be considered as the physicians of the computer system, also we can call them the pathologist or better still the cardiologist of the computer system. Let‘s not under-estimate the impact of security incidents, which can lead to data loss, leaks of personal information, wasting of time, and the spread of viruses. We shouldn’t’ think that security incidents that happen to other computers will not affect us. We should take responsibility in managing your own information. Keep alert to news regarding security threats and equip ourselves and organizations with the latest knowledge. Consult experts and advisors if you are in any doubt. Keep a contact list of assistance, e.g. public services, application support, and ISP hotlines.

Keywords: Defending information from unauthorized access; Key to the future of every organization.

1. Introduction

Information security is of great importance and interest to everybody in the world of technology today, whether you are a mobile phone or a personal computer user, this is why information security is of the most importance in our everyday life, and in the IT technology fields.

---

* Corresponding author.

The Study of information security has so many concepts and also topics that every IT professionals should master or have some basics of, the knowledge and skills of information security are just some few that is essential for all those that are involved in the IT technology sector. E.g. Cyber-security analyst, forensics analyst, network administrators, systems administrators, application developers. Lack of knowledge in this important field of information security will be more likely to develop applications that are not secure or build networks that are insecure and easier for attackers to penetrate, this is why information security knowledge is very important in our everyday lives. Regardless of the choosing career, you find yourself in the IT technology sector.

2. Organizational Security policy

There is the need for an organization's information security policy, this should not simply convey a plan of action, for example, its purpose, goals, applicability, importance and activities; most importantly organizations should also document who is ultimately responsible for carrying out the security agenda across the enterprise [14]. All personnel within the organization should be provided in the appropriate training on information security policy and the organization's security expectations, aligned to their functional roles. As an example, the corporate internet usage policy should be communicated in a clear manner, read, understood and acknowledged by all personnel within the organization, while a role specific policy such as the enterprise software management policy, should be scoped to include all the relevant personnel, for example, the IT Systems department. It is also imperative for organizations to track dissemination of policies and procedures through employee attestation, as this helps provides a valuable input into policy enforcement and education processes.

3. Network Security benefits

The 2009 FloCon conference3, security analysts were given demonstrations of the FloVis framework for network visualization, including all three plug-ins [6]. During this demonstration, they identified a need for highly abstracted visualizations of network structures and their related communications that would assist the user with determining those subnets/hosts that should be visualized with the existing plug-ins. For instance, network analyst/systems engineers may be responsible for monitoring several departments and may be aware of outside networks, subnets, and/or individual host Internet Protocol (IP) addresses that pose a threat to the security of the departments. Thus, it would be beneficial to provide a high-level visualization of the relationship between these "organizations" before deciding what to visualize at a lower level. A common practice in IS research is to treat information systems themselves as either a dependent variable or an independent variable. Accordingly, IS frameworks usually attempt to classify information systems in one of two ways. Firstly, systems can be classified based on technical attributes. For example, characterizes information technology in terms of its capacity, quality, cost, storage, processing, and communications capabilities. It is also possible to classify computing arrangements as interactive versus batch standalone versus networked, and so on. The second approach is to focus on the functions information systems perform within their context of use and whose interests are served by information technology. For example, Markus identifies five types of information systems, each describing a dominant type of function: operations, communication, planning and decision-making process, monitoring, evaluate and control, and inter-organizational transactions. The Gorry and Scott Morton framework also build its classification of information systems upon functional differences rather than

technical attributes. K analysis indicated a real gap in knowledge in terms of ISM studies in developing countries. The literature analysis could not identify any papers that included holistic frameworks or articulated a complete model showing all the factors that aid the implementation and adoption of IS culture. However, the 68 papers did reveal a range of issues and factors that influence IS culture and some of the practices. These factors included: Information Security Awareness, and Training Programs, ISM Standardization, Information Security Policy, Top Management Support for ISM, Information Security Compliance, Information Security Risk Analysis, and Organizational Culture. These issues were classified into the following themes, each of which is discussed further below

- Corporate citizenship
- Legal regulatory environment
- Corporate governance
- Cultural factors, However, in the case of Saudi Arabia, national cultural factors tend to be some of the obstacles and can affect the adoption of IS cultural and practices in Saudi Arabian organizations. Therefore, this study will examine the importance and influence of ISM factors and cultural factors on the adoption of IS cultural and practices in Saudi Arabia.

4. Why network or Systems security

The system and network technology is a key factor in information technology for a wide variety of applications. Security is crucial to networks and applications. Although network security is a critical requirement in most emerging networks, there is a significant lack of security methods that can be easily implemented to ensure maximum security. There exists a “the communication gap” between the developers of security technology and developers of networks. Network design is a well-developed process that is designed based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing the networks. It offers modularity, flexibility, ease-of-use, and standardization of the network protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making any other adjustments, allowing flexibility in its development. In contrast to network design, secure network design is not a well- developed process. There isn’t a methodology to manage the complexity of security requirements. Secure network designs do not contain the same advantages as network design. When considering network security in the organization, it must be emphasized that the whole network is secure and can offer the security required. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel and cause harm, obtain the data, decrypt it and re-insert a false message. Securing the network is just as so important as securing the computers and encrypting the message. When developing a secure network, the following should be considered:

1. Access – authorized users are provided the means to communicate to and from a particular network

2. Confidentiality – Information in the network remains private to trusted staff or users.

3. Authentication – Ensure the users of the network are who they say they are.

4. Integrity – Ensure the message has not been modified in transit and is secured during transmission.

5. Non-repudiation – Ensure the user does not refute that he/she used the network

Let's take the example a website there are various factors involved in drawing visitors to your site, network and turning them into customers, it's extremely important that you enlist the help of proficient webmasters and security experts to manage your site and secure the network.

It is time to take serious information security measures in our organizations, prevent common internet attacks. Some of the measure that can be taking to prevent that the networks are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing.

Attacks can also interfere with the system's intended function, such as viruses, worms, and trojans. The other form of attack is when the system's resources are consumed uselessly.

Eavesdropping. Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted.Sensitive information can be stolen through eavesdropping.

Worms

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate [9]. There are two main types of worms, mass mailing worms, and network-aware worms. Mass mailing worms use email as a means to infect other computers. Network aware worms are a major problem for the Internet.A network aware worm selects a target and once the worm accesses the target host, it can infect it by means of aTrojan or otherwise.

Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus.

Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP spoofed packets cannot be eliminated.

Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestor. The system then consumes resources waiting for the handshake to complete. Eventually, the system can not respond to any more requests rendering it without service.

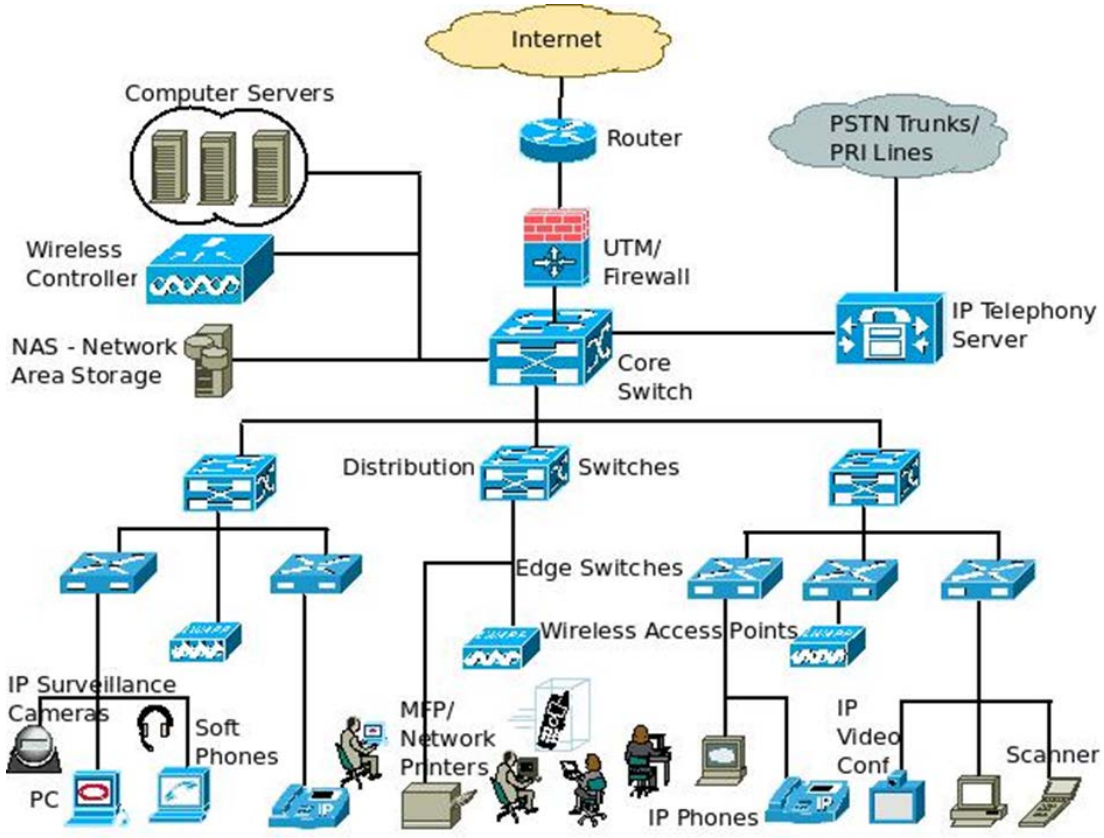

Figure 1: Organizational Network Architecture

No matter how attractive your site looks like, looks alone are not enough to generate sales. Rather than entrusting your website to inexperienced service providers who may not have a full range of webmaster Skills, without basic knowledge of information security, the webmaster or web developer is very likely to design or program a website that will easy to for attackers to penetrate.

5. T Security Knowledge for Database Administrators

Database administrators are responsible for the management of our database servers in the organization,

databases are used to store our valuable information in the organization's database. There is growing evidence that descriptor-driven machines provide an excellent base for constructing penetration proof operating systems, although it is clear that even with such aids it is necessary to exercise care in the implementation of the operating system. Information security is hardly a new concept. The need to protect valuable information is as old as mankind. Whether that information was the location of a rich hunting ground, a technology for producing weapons, or a knowledge of the divine, it had value and therefore needed protection. Today, information security is often conceptualized as being the protection or preservation of four key aspects of information: availability, integrity, authenticity, and confidentiality. Availability: Accessibility of information for a purpose. Integrity: Completeness, wholeness, and readability of information, and the quality of being unchanged from a baseline state. Authenticity: Validity, conformance, and genuineness of information. Confidentiality: Limited observation and disclosure of knowledge to only authorized individuals.

Many professionals have given lots of insight into the core function of a database administrator, one of them is the management of data, With all storage references interpreted by descriptors, it is possible to more effectively apply for selective permissions (read, write, execute, etc.) to different parts of the operating system. Third, the portion of the operating system dealing with real resources (memory, peripherals, file space, etc.) can be localized and made as secure as need be for securing the system. Finally, descriptor-driven (virtual) machines make it possible to include the operating system in the user's address space in a protected way, thus facilitating intra-process communication, and enforcing separately the controls for reading (data or programs), writing and execution. but some organizations define different functions for the Data Administrator than those of the Network Administrator. Database Administration concerns the responsibility for serving as the custodian of the firm’s data. A basic premise for intrusion detection is that when audit mechanisms are enabled to record system events, distinct evidence of legitimate activities and intrusions will be manifested in the audit data. Because of the sheer volume of audit data, both in a number of audit records and in the number of system features (i.e., the fields describing the audit records), efficient and intelligent data analysis tools are required to discover the behavior of system activities.

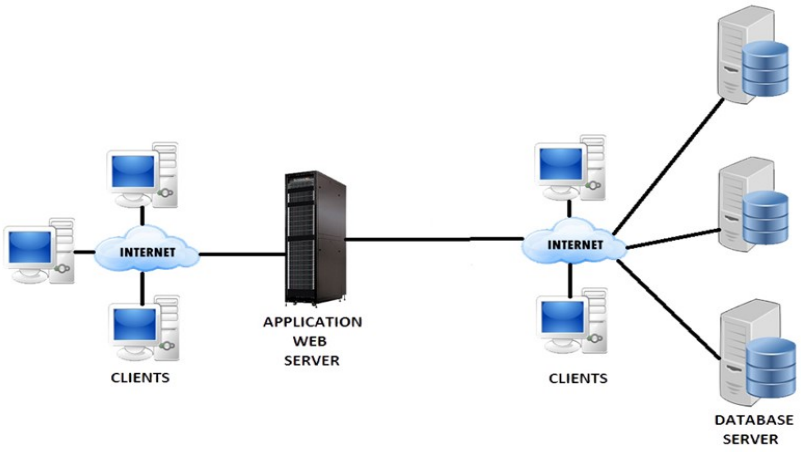

Figure 2: Database Security Architecture

The Data Administrator: resolves disputes that arise because data are centralized, but shared among system

users. Decides where data will be stored and managed, Maintains corporate-wide data definitions and standards, Plans for database usage, analysis, design, implementation, maintenance, and protection. Has a high level of both managerial and technical skills.

❖ Database Administration involves the actual hands-on, physical management of databases. This is a very technical function that focuses on physical database design issues including security enforcement, system performance, and backup/recovery. I know this may sound confusing. There is a difference between a Data Administrator and Database Administrator:

❖ A data administrator (also known as a database administration manager, data architect, or information center manager) is a high-level function responsible for the overall management of data resources in an Organization. In order to perform its duties, the DA must know a good deal of system analysis and Programming.

❖ These are the functions of a data administrator (not to be confused with database administrator functions): Data policies, procedures, standards

❖ Planning- development of organization's IT strategy, enterprise model, cost/benefit model, the design of database environment, and administration plan.

❖ Data conflict (ownership) resolution

❖ Data analysis- Define and model data requirements, business rules, operational requirements, and maintain corporate data dictionary Internal marketing of DA concepts Managing the data repository.

❖ Database administration -is more of an operational or technical level function responsible for physical database design, security enforcement, and database performance. Tasks include maintaining the data dictionary, monitoring performance, and enforcing organizational standards and security. There is also the database steward, Database stewards- are the people with administrative function responsible for managing data quality and assuring that organizational applications meet the enterprise goals.It is a connection between IT and business units. Data quality issues include security and disaster recovery, personnel controls, physical access controls, maintenance controls, and data protection and privacy. Data mining generally refers to the process of extracting useful models from large stores of data.The recent rapid development in data mining has made available a wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and databases. Several types of algorithms are particularly useful for mining audit data: The importance of information security in a computer-based environment has resulted in a large stream of research that focuses on the technical defenses (e.g., encryption, access control, and firewalls) associated with protecting information.

❖ For example, in order to increase security, the database steward can have control over who can gain access to the database by assigning a specific privilege to users. Deterrence employs disciplinary action to influence human behavior and attitude. When applied within organizations, the effectiveness of deterrence is influenced by two key factors – certainty of sanctions and severity of sanctions. The certainty of sanctions (i.e., the probability of being caught) is influenced by the level of awareness of the kind of sanctions, as well as the ability to enforce bodies to detect offending behavior. The severity of sanctions is influenced by the range of sanctions that can be imposed.

6. CIA in Information Security (C: Confidentiality, I: Integrity, A: Availability)

Does the name CIA or term sound familiar, the core function of the CIA. (Central Intelligence Agency) is a civilian foreign intelligence service of the U.S. Government, tasked with gathering, processing and analyzing national security information from around the world, primarily through the use of human intelligence. Is an arm of the United States secret Service, in fact, a very important arm of The United States secret service o better still one of the most respect security institution in the world? Well in a computer or information security(CIA) in computer terms or in information security is known as:

Figure 3: CIA Architecture

Confidentiality

Well anybody body who is abreast with the works of the US secret service, knows the core functions of the CIA in the united states well these concept in Information security means having confidence in something, and logically we all know what having confidence in something means, in simple terms it means trusting in the person or a thing. so in information security cycles , confidentiality is to make or ensure that only trusted people are seeing or accessing the information and ensuring that the confidence of the information is maintained Confidentiality- has a lot to do with technology, that helps protect data and also to ensure only the right or trusted people have access to the data. And how do to ensure or be assured that the people we so much trust will not turn against us or abuse the trust we have in them. This is where integrity comes in, it means we should be sure that the person we so much confidence in, is someone or is a person that has integrity and someone that stand up to his words committed individual that is committed to his/her work, this is the same with computer security, it will always be what we knew it to be now or at later time when we return to access the data.

Integrity helps ensure that our data is what it's supposed to be, anytime we need it, this is where availability comes in. A basic premise for intrusion detection is that when audit mechanisms are enabled to record system events, distinct evidence of legitimate activities and intrusions will be manifested in the audit data. Because of the sheer volume of audit data, both in a number of audit records and in the number of system features (i.e., the

fields describing the audit records), efficient and intelligent data analysis tools are required to discover the behavior of system activities. Data mining generally refers to the process of extracting useful models from large stores of data. The recent rapid development in data mining has made available a wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and databases. Several types of algorithms are particularly useful for mining audit data:

Confidentiality is the term used to prevent the disclosure of information to unauthorized persons individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the place where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality.

Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

CIA thus Confidentiality, integrity, and availability. This word keeps being discussed throughout when discussing information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction [1].

Integrity

In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised.Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.Others have found that deterrence efforts have a positive effect on information security.recommended that organizations should increase training in security policy compliance and should focus on policing policy breaches.

Availability

For any information system to serve its purpose, the information must be available

when it is needed. This means that the computing systems used to store and process the

information, the security controls used to protect it, and the communication channels used

to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

Computer Emergency Response Team

Computer Emergency response Operations and Incident Command The Emergency Operations and Incident Command unit works closely with the SOC. The primary responsibility of this unit is to mobilize staff, activate response plans, and manage time-critical incident management and response activities when a high-impact incident is declared. During normal operations, this unit conducts the following activities in concert with members of the SOC:

- planning for incident management and response
- planning for business continuity
- intrusion detection
- planning for IT disaster recovery
- prevention and ensuring maximum security
- performing tests, exercises, and drills of all response plans
- performing problem management, root cause analysis, and post-mortem reviews following the occurrence of an incident
- conducting forensic investigations and working with law enforcement and other regulatory bodies during and following an incident.

The main challenges of defining security metrics information technology lie the problem that metrics must be quantifiable information (like percentage, average or even absolute numbers) for comparison, applying formulas for analysis and tracking the changes [7]. The result from the manual collection or automated resources should be meaningful to the performance data and must be based on IT Security performance goals of the organization. Metrics should also be easily obtainable and feasible to measure and should not be compromised. But research methodology plays an important role here, not to have biased data as a result; and to cover all dimensions of IT security from organizational (people), technical and operational points of view. Concerning these conditions, the

problem is to set standardized quantitative IT security risk metrics for efficient evaluation of IT security performance.

The objective of the risk management system is permanent risk reduction, protection of sensitive resources, systems and processes, as well as protection against any potential effects of such risks. The risk management system should allow retrospective evaluation of the efficiency of actions undertaken with

respect to:

- business process of the organization,
- employees and users in the organization,
- appropriate technologies.
- The main tasks of the system include:

The provision of the information about risks and their profiles;

• the performance of preventive actions reducing the risk and its consequences;

• monitoring of the acceptable risk level and finding long-term mitigation measure or preventive measures

The elements of the operational risk management system of the organization are the following:

•The strategy and policy rules of the organization with respect to risk management;

• by-laws and procedures defining the risk management process.

7. Network Cryptography

Network cryptography is based on the effects that two or more neutral networks are able to synchronize by their mutual learning. In each and every step of the online procedure, these enable it to get common input patterns and calculate their outputs.then both neutral networks are those that use the outputs, presented by their adjustable weights.

8. Concept of Triple

In computer security, AAA(Triple A) known as authentication, authorization, and accounting. These refer to a security architecture for distributed systems that enables control over which users are allowed access to which or what kind of services and that keeps tabs on how much of the resources they have used. Two network protocols providing this functionality are particularly popular.

- **Authentication**- refers to the process where an entity's identity is authenticated, typically by providing an evidence that it holds a specific digital identity or personal identities, such as an identifier and the corresponding credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, digital signatures, and phone numbers (calling/called).then helps control, who has access to our systems and

whatever it's in the machine, and it works with the help of authentication, when our authentication is weak, whatever the machine authorizes will be useless or will be very weak and can be compromised, so authorization depends on authentication before it can function properly, when the system or the machine, it's very easy for hackers to attack, by just guessing the password and getting access to the data on the machine.

Authentication is what helps identify the identity of an individual, and not only that, it helps protect our machines and our personal selves until it's certain or verifies the true identity of the Individual.

- **Authorization -**Usually occurs within the context of authentication. Once you have authenticated a user, They may be authorized for different types of access or activity or consenting for an action in the system. The final plank in the AAA framework is known as accounting, which measures the resources a user consumes during access on the system. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistical usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity, and planning of activities.
- **Accounting**- This accounting is not the accounting we know in financial terms, or in financial world, in information security (IT) this is referring to watching what other people do on our network, things they access, when they accessed it, from where they access it, are they running other programs on the machines, like programs that will allow them to sit in another location and steal our valuable data. Or reading confidential documents on the systems, or also if the person is creating a new file or modifying a File, this is the accounting that goes on within the computer system, it is for this reason that it's sometimes referred to as Auditing. Because it performs the functions of audits of whatever is going on the system, be it a single system, or many systems on the network some expert also said the first process in (AAA), The authorization functions and determines whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service. Authorization may be determined based on a range of restrictions, for example, time-of-day restrictions, physical location restrictions, or restrictions against multiple access by the same entity or user. Typical authorization in everyday computer life might be, for example, to grant reading access to a specific file for an authenticated user. Examples of types of service include but are not limited to: IP address filtering, address assignment, route assignment, quality of service/differential services, bandwidth control services /traffic management, compulsory tunneling to a specific endpoint, and encryption.

Authentication provides a way of identifying a user, typically by having the user enter a valid username and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication and credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied. Following the authentication, a user must gain authorization for doing certain tasks. After logging into a System, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing the policies on the system: determining what types or qualities of activities, resources, or services a user is permitted.

Many systems on the network some expert also said the first process in (AAA), In AAA parlance, the term "provisioning" refers to communicating a user's session rights and constraints to the PEP so that the PEP can grant and enforce these permissions [11]. One of the most difficult aspects of provisioning access rights on a PEP is communicating the decision of the PDP in a format the PEP can understand. This fact is one of the reasons that many PEPs come with a lightweight PDP. This approach solves the narrow problem for that PEP but creates management challenges when coordinating network AAA across a broader enterprise, because the enterprise AAA policies must be implemented individually on each unique type of PEP on the network. Because RADIUS is the most commonly used network AAA protocol, it is natural to communicate the PDP decision using that protocol. RADIUS attributes such as the "filter-id" allow the PDP to trigger a preexisting filter on the PEP.

Usually, authorization occurs within the context of authentication. Once you have authenticated a user, They may be authorized for different types of access or activity. The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistic and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

9. Least Privileges

UAC in Microsoft windows Vista and Windows 7 includes many improvements that make it easier to work without administrative privileges and helps overcome many of the problems faced by users when removing administrative privileges from the system [10]. Microsoft also has a free tool called theApplication Compatibility Toolkit (ACT) that can be used to deploy and fixes for applications not compatible with LUA. Though removing administrative privileges from users' accounts is simple from a technical perspective, it can result in a series of problems:

Ensures that the user is not given more capabilities than required to perform his or her responsibilities. Also known as the principle of minimum necessary access.

A capacity is a capability or a permission, functions, rights, things that they are allowed to do. Each user or process has a responsibility. Let's take, a company CEO, has the responsibilities of his company's financial matters, and so in that case, so that person should be given the rights to all financial data, so in this case the duties of function or the financial officer doesn't include the checking the email because he or her not or does not have that permission. The duty is only to handle the financial matters of the company. And not the management of the email server or checking the staff emails of the company. Least privileges are enforced through proper permission management. Discretionary Access control: when properly implemented is in compliance with least privilege, so discretionary access control is used in deciding what people can access. In simple terms, we can call it controlling what is accessed on the network, and not everyone can access everything but can access what is granted to them, things they need to access. the application of 'least privilege' applies to people, process, and technology. For people at your organization, this application typically targets the role or function that they have, and looks to implement 'separation of duties'. In most cases, this idea is understood and

well implemented in financial organizations because they must follow strict guidelines and have their controls regularly audited. Similarly, the financial department at any organization will often implement 'separation of duties' for financial functions. For example, most organizations have separate functions associated with initiating a payment and authorizing payment, as a common practice. The goal is to reduce opportunities and the risk of intentional or accidental misuse of systems or information.

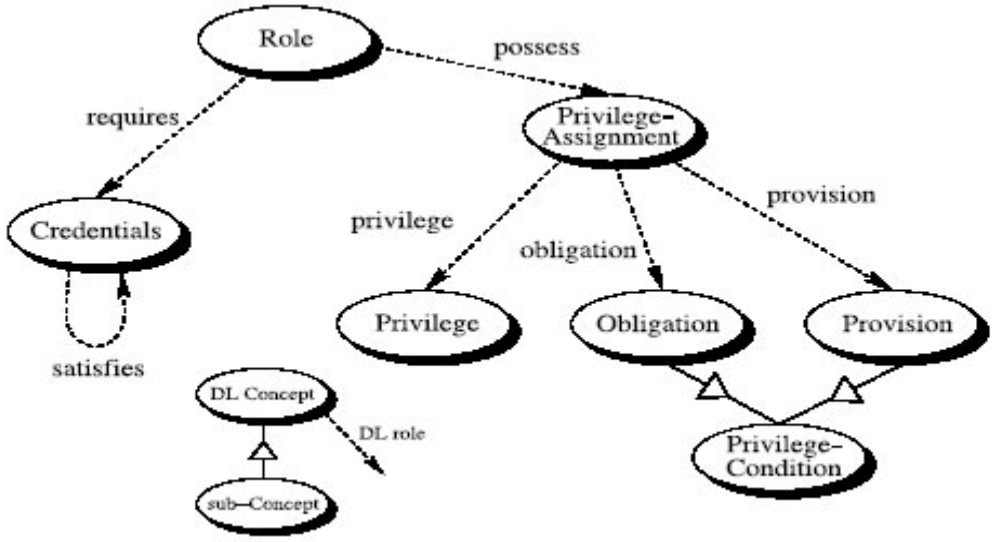

Figure 4: Authorization policy model

Availability: Accessibility of information for a purpose. Integrity: Completeness, wholeness, and readability of information, and the quality of being unchanged from a baseline state. Authenticity: Validity, conformance, and genuineness of information. Confidentiality: Limited observation and disclosure of knowledge to only authorized individuals.

10. Surface Attacks

A typical attack surface has complex inter-relationships among three main areas of exposure: software attack surface, network attack surface, and the often-overlooked human attack surface. The same way, if that machine is on a network, the attack points can be the points, e.g. if the machine is on the web server, it can easily be attacked through the port 80 [16]. If the machine is on the SMTP server it's easier to also gain access to the SMTP services, same with active directory services (LDAP) lightweight active directory protocol. The first and most prominent attack surface is that of a service instance towards a user. This is nothing else than the common server-to-client interface, thus enabling (and being vulnerable to) all kinds of attacks that are possible in common client-server-architectures as well. This involves things like buffer overflow attacks, SQL injection, or privilege escalation [12]. In the same way, the attack surface the service user provides towards the service is nothing else than the common environment a client program provides to a server, e.g. browser-based attacks for an HTMLbased service like SSL certificate spoofing.

But the good news is that there is a way we can minimize or reduce the impact of the attack when it occurs on

the machine. By simply using attack service reduction, by disabling unneeded services, so we can also do that by simply using a firewall to block the port, though the application might be running on the machine. Another simplest way is to just disconnect the machine from the network. These are the some of the methods used in preventing some Attacks on our network. Even if it happens it will be minimal. Situational awareness enables security decision makers to better cope with information security incidents and develop more effective defenses Combined points through a system may be attacked. E.g. keyboards, mouse, USB Ports, CD/DVD drives, external drives, firewire and etc. this are able to allow a person to the physical machine. Your attack surface is the sum of your security risk exposure. Put another way, it is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks. A smaller attack surface can help make your organization less exploitable, reducing risk.

11. Conclusion

We should take responsibility in managing your own information and security, and also take steps to Protect and secure our data, and help build the capacities of those responsible for the security and investments of our organizations, with the world moving at a faster pace, so are hackers, like Script Kiddies, these kind of cyber criminals normally don't care about hacking. And the other cyber thieves, that exploit on people's ignorance on information security issues.Information security will make the world a better place for all. And prevent all people in this world from using the computer and the Internet to hurt innocent people.Information security is

Acknowledgement

Our greatest thanks go to Professor, Han Jian Min of Zhejiang Normal University. College of Mathematics, Physics and Information Engineering for his excellent supervision and guidance, skills, help, and importantly

guiding us through each and every step of the process with knowledge and support, Thank you for very much your advice. We will always remain grateful. It has been an honor to study under your guidance.

12. Recommendations

Based on the conclusion above and from the topics Information Security in an Organization the following are recommended;

i. Situational awareness enables security decision makers to better cope with information security incidents and develop more effective defenses [4].
ii. Organizations should increase training in security policy compliance and should focus on policing policy breaches [3].
iii. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction [1].

13. Support

This work is supported by National Natural Science Foundation of China under Grant 61672468.

References

[1.] Sattarova Feruza Y. and Prof.Tao-hoon Kim, IT Security Review: Privacy, Protection, Access Control, Assurance and System Security, International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, (2007) page 17

[2.] JAMES P. ANDERSON, computer security technology planning study, ESD-TR-7315 Vol. II (October)1972.

[3.] Artail H, Safa H, Sraj M, Kuwatly I, AlMasri Z. A hybrid honeypot framework for Improving Intrusion detection systems in protecting organizational networks. computers & security 25:. (2006):274288.

[4.], Lakkaraju K, yurcik W, are H, A visualization tool for situational awareness of tactical and strategic security(2003) ents on large and complex computer networks. paper presented at the military communications conference (MILCOM).

[5] Ferguson, N., Schneier, B., Kohno, T. 2010 Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing ISBN:0470474246 9780470474242.

[6] D. Paterson, T. Taylor, S. Brooks, J. Glanfield, C. Gates, and J. McHugh. Activity Plots: A Multi-Entity Time Series Visualization. In Online Proceedings of FloCon 2009. URL: http://www.cert. org/flocon/2009/proceedings.html, January 2009

[7] U.S. Department of Homeland Security US-CERT Cyber Resilience Review website, September 2015.Retrieved from https://www.us-cert.gov/ccubedvp/self-service-crr

[8] Gorry GA. and M.S. Scott Morton, A framework for management information systems. Sloan management review, 13(1): P. (1971.):5570.

[9] Dr. Rajinder Singh, Shakti Kumar, NETWORK SECURITY & VULNERABLE SECURITY ASPECTS, global journal of engineering science and researches Singh, 1(6): August 2014] ISSN 2348 8034

[10] Avecto | Whitepaper, Regulatory Compliance and Least Privilege Security. Retrieved from HTTP:// www.avecto.com.

[11.] Rigney et. al., "Remote Authentication Dial In User Service (RADIUS)," RFC 2865 (Obsoletes RFC 2138, 2058), June 2000.

[12.] Nils Gruschka, Meiko Jensen. Attack Surfaces: A Taxonomy for Attacks on Cloud Services, Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing.

[13]. Siponen . "Neutralization: New insights into the problem of employee systems security policy

violations," MISquarterly, 2010.:(34: 3) pp.487502

[14] Julia H. Allen, Structuring the Chief Information Security Officer Organization, September 2015.

[15] Cavalli, Richard A.; Allen, Julia H.; & White, David W. CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience. Addison-Wesley, 2011. http://www.informit.com/store/cert-resilience-management-model-cert-rmm-a-maturity-9780321712431.

[16] Katherine Brocklehurst, RISK-BASED SECURITY FOR EXECUTIVES, white paper, Understanding Your Attack Surface: The First Step in Risk-Based Security Intelligence, APR 17, 2014